Defense Information Systems Agency
A Combat Support Agency

DoD Information Assurance Certification and Accreditation Process (DIACAP)

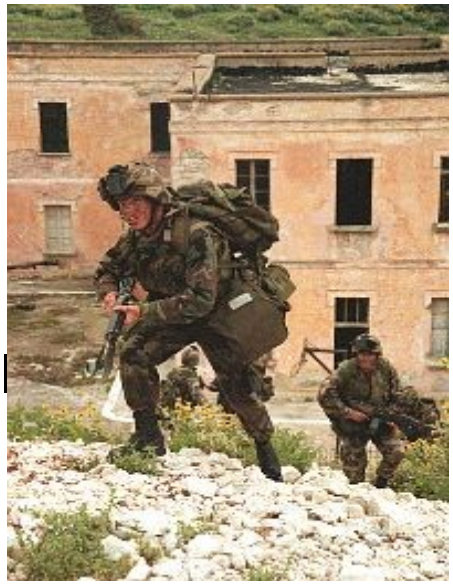
August 2011

DISA
A Combat Support Agency

Our Goal……Protecting DISA's Networks At Sea and On Shore

DISA
A Combat Support Agency

What are we protecting?



- **DOD Information**
  - **Classified Info**
  - **Privacy Act Info**
  - **Sensitive but Unclassified/Nuclear I**
  - **FOUO (For Official Use Only)**
- **Systems**
  - **C4 (Command, Control, Communication & Computer) Systems**
  - **POR (Program of Record) Systems**
- **Networks**
  - **NIPRNET (Unclassified)**
  - **SIPRNET (Classified)**

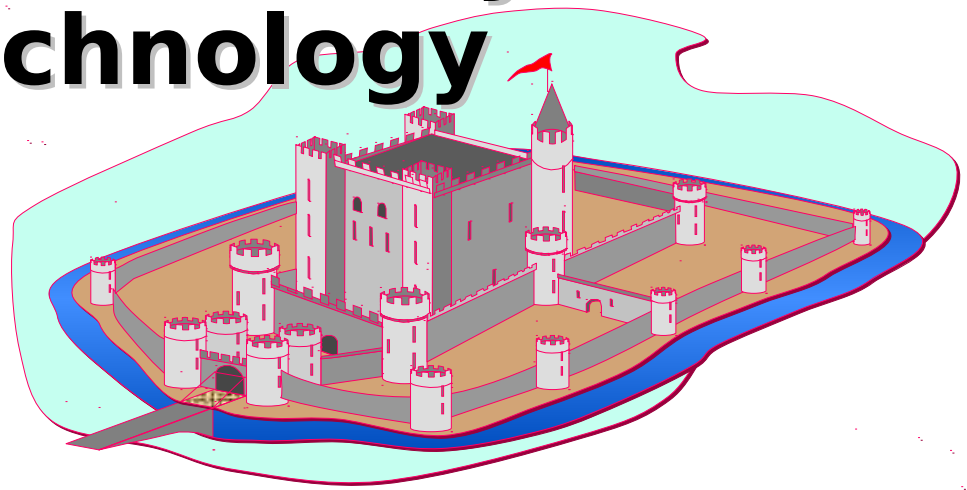
DISA
A Combat Support Agency

What are we protecting from?

- **Insider Threat (Often under-estimated)**
  - Disgruntled personnel
  - Unintentional actions of user
  - Trusted insider ???
- **Hacker/Cracker**
- **Malicious Code/Viruses/Worms**
- **State Sponsored CNA (Computer Network Attack)**
- **DOS (Denial of Service) Attacks**
  - Self imposed
  - Deliberate actions of others

DISA
A Combat Support Agency

Defense-in-Depth: It's more than just technology



- Right people in the right job
- Training, Training, Training
- Tactics, Techniques, and Procedures
- Hardened infrastructure
- Layered Protection
- Right DiD tool/technology in the right layer

DISA
A Combat Support Agency

Certification and Accreditation

- **DIACAP = DOD Information Assurance Certification and Accreditation Process**
- **Designated Approval Authority (DAA)**
  - **Active Involvement**
  - **Risk Management**
- **Program Manager (PM)**
  - **Ensures Security Design**
- **Certification Authority/Agent (CA)**
  - **Reviews package/supports PM in design and verification**
- **Risk Management Framework (RMF)**

DISA
A Combat Support Agency

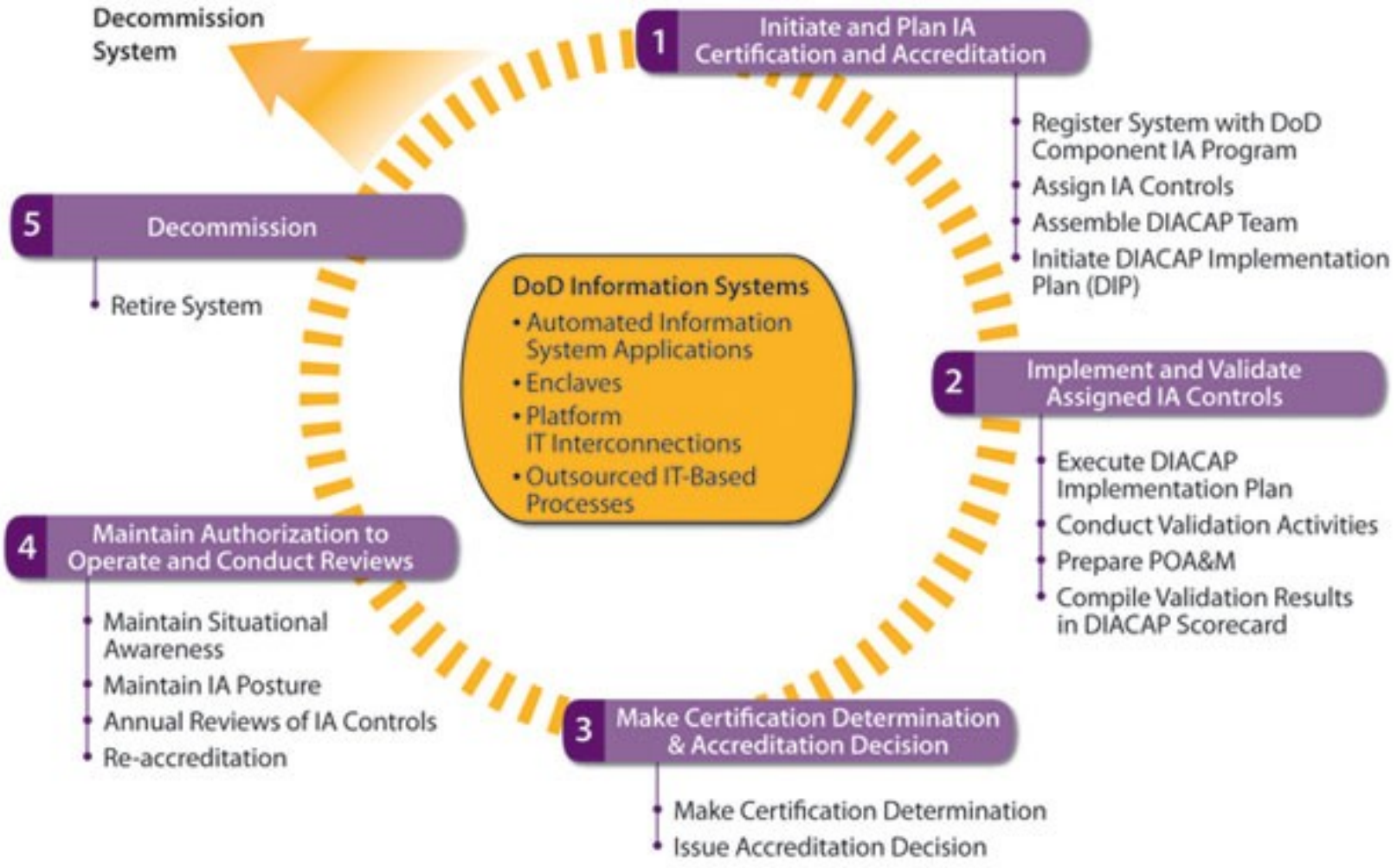
Phase Description

- **DIACAP melds into a “Lifecycle” support scheme very well**

- **Re-assessment of security posture/compliance and ATO status no less than once per year**

DIACAP Lifecycle Phases of an IT System

A Combat Support Agency


Decommission System
1 Initiate and Plan IA Certification and Accreditation
Register System with DoD Component IA Program
Assign IA Controls
Assemble DIACAP Team
Initiate DIACAP Implementation Plan (DIP)
2 Implement and Validate Assigned IA Controls
Execute DIACAP Implementation Plan
Conduct Validation Activities
Prepare POA&M
Compile Validation Results in DIACAP Scorecard
3 Make Certification Determination & Accreditation Decision
Make Certification Determination
Issue Accreditation Decision
4 Maintain Authorization to Operate and Conduct Reviews
Maintain Situational Awareness
Maintain IA Posture
Annual Reviews of IA Controls
Re-accreditation
5 Decommission
Retire System
DoD Information Systems
• Automated Information System Applications
• Enclaves
• Platform IT Interconnections
• Outsourced IT-Based Processes

Source: http://www.prim.osd.mil/cap/dhra-diacap.html?p=1.1.1.1

DISA
A Combat Support Agency

DIACAP Tools

- **DIACAP Packages are created with the help of:**

- **Knowledge Service (KS) – DoD-wide web based database of C&A efforts**
- **Enterprise Mission Assurance Support System (eMASS) – automates management functions**

DISA
A Combat Support Agency

DIACAP KS

- **Provides DIACAP process information**
- **Implementation Guides**
  - **Central point for process data dissemination**
  - **C&A News**
  - **Updates to controls**
  - **Generic Forms/Templates**

DISA
A Combat Support Agency

eMASS

- **Aids document production**
  - **Automates status reporting, workflows, artifact creation**
- **Acts as storehouse for infrastructure documents**
  - **Tracks all enterprise systems**
  - **Links C&A efforts across organization**

DISA
A Combat Support Agency

DIACAP Executive Package

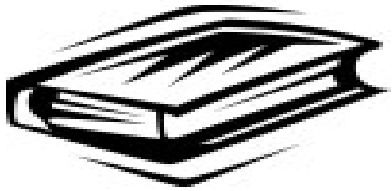
- **Minimum information <u>for accreditation decision</u>**
  - **System Identification Profile**
  - **Scorecard**
  - **Certification Determination**
  - **POA&M**
  - **Accreditation Decision**

DISA
A Combat Support Agency

Comprehensive Package

Comprehensive Package

- **System Identification Profile**
- **DIACAP Strategy**
- **Implementation Plan**
- **Security Control Requirements**
- **Relevant Artifacts, Validation Procedures, etc.**
  - **Scorecard**
  - **Certification Determination & Artifacts**
  - **POA&M**
  - **Accreditation Decision**



System Identification Profile (SIP)

A Combat Support Agency

- Initial product of the DIACAP
- Describes Mission and System for Review
- Specifies DIACAP Team Members
- Formal System Registration
- Determination of MAC and CL

DISA
A Combat Support Agency

Implementation Plan

- **Relevant Security Controls**
- **Lifecycle Analysis**
- **Configuration Description**

Once the Implementation Plan is set, its execution kicks off the Validation Process

DISA
A Combat Support Agency

Validation & POA&M

- **System Tests/Test Plan**
- **Validation results**
- **POA&M with discrepancies**

Note that these are completed prior to the formal Scorecard creation

DISA
A Combat Support Agency

DIACAP Scorecard

The Scorecard shows the certification status of a system in a concise format

Displays:

- **Number of Controls Required**
- **Number of Compliant/Non-compliant Areas**
- **Assessed Risk Status of Each Non-compliant area**

DISA
A Combat Support Agency

Certification & Accreditation Decisions

- **DIACAP Package + Risk Assessment Presented to the Certification Authority (CA)**
- **CA issues Certification Recommendation (Cert Rec)**
- **DAA Takes the CA recommendation and DIACAP Package to Make Accreditation Decision**

DISA
A Combat Support Agency

Authority To Operate

Accreditation Decision takes the Form of:

ATO – Authority to Operate (NO provisions)

IATO – Interim ATO (provisions set forth in POA&M required)

IATT – Interim Authority To Test (inside given timeline only)

DATO – Denial of ATO (Reassess Implementation Plan…)

DISA
A Combat Support Agency

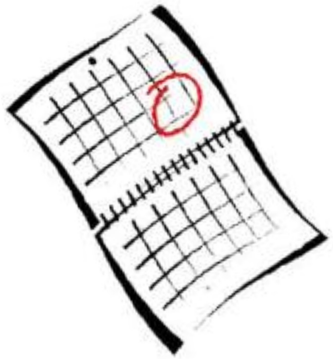
ATO Maintenance

- **Monitor IA-Relevant Issues (vulnerabilities, exploits, policy changes, best practices, etc.)**
- **Conduct Annual Reviews**
- **Complete Re-Accreditation Process**
  - **(3 Years)**

DISA
A Combat Support Agency

ATO Maintenance (cont)

- **Correct newly discovered CAT I weakness within 30 days**
- **Correct newly discovered CAT II weakness within 90 days**
- **Continued ATO is contingent on the sustainment of an acceptable IA posture**
- **Identify Decommission Point**



C&A Timeline

- **30-60 days out from expiration date**
  - **Notification via IA Compliance Slides**
- **30 days out**
  - **Cert Rec & DIACAP Package du**
  - **Time to work out any issues**
- **5 days out**
  - **DAA review**
- **Connection Approval Process (CAP)**
  - **Circuits**
  - **Requires 21 days to process**

DISA
A Combat Support Agency

Questions?

- **DIACAP Knowledge Service (https://diacap.iaportal.navy.mil)**
- **CIO-IA-Security (cioiase@disa.mil)**
- **Ref: DoDI 8510.01**